様式 C-7-2

自己評価報告書

平成２３年　４月２２日現在

機関番号：８２６２６
研究種目：若手研究（Ｂ）
研究期間：2008～2011
課題番号：２０７０００１７
研究課題名（和文）　隠れ部分群問題に対する効率的量子アルゴリズムの構築可能性の分析

研究課題名（英文）　Analysis of possibility of efficient quantum algorithms for Hidden Subgroup Problem

研究代表者
縫田　光司（NUIDA KOJI）
独立行政法人産業技術総合研究所・情報セキュリティ研究センター・研究員
研究者番号：２０４３５７６２

研究分野：数学、情報セキュリティ
科研費の分科・細目：情報学・情報学基礎
キーワード：量子情報理論、応用数学

１．研究計画の概要

本研究では、量子アルゴリズム分野の主要問題である隠れ部分群問題が、量子計算機実現後の暗号系の信頼できる安全性基盤たり得るか否かについて、新たな視点からのアプローチも加えた多角的な研究によってより強い傍証を与えることを目的とする。

２．研究の進捗状況

これまでの研究では、まず、量子アルゴリズムの構築および性能評価に有用と期待される数学理論および量子情報理論の調査および整備を行った。具体的には、量子アルゴリズムと密接な関係のある量子状態識別問題について、幾何学的なアプローチを用いることで、状態識別の理論的な最適成功確率の見積もりに有効な新たな手法を考案した。また、量子アルゴリズムの性能評価の基盤となる量子情報理論における中心的な概念である（量子）エントロピーについて、既存の数学的定式化を更に抽象的・操作論的な観点から再検討することにより、いくつかの既知の性質に対する新たな解釈を提示するとともにいくつかの未知の性質を見出すことに成功した。更に、量子アルゴリズムを実装する量子計算機の最小記憶素子の候補と考えられている２準位量子系（キュービット）について、ある物理系がキュービットとして振舞うための必要充分条件を、その物理系が満たすべき物理原理の族を記述する形で明らかにすることに成功した。これらの研究においては、研究代表者の数学的バックグラウンドを活かした数理科学的考察に加え、数学および物理学の専門家との意見交換を定期的に行うことにより、多角的な研究視点を確保することに注意を払った。

これらの成果に基づく隠れ部分群問題の考察として、まず隠れ部分群問題に関する既存の研究についてその理論的特徴や改善が望まれる点の整理を行い、シンポジウムにおいて発表することで参加者からの専門的フィードバックを得た。その調査結果に基づく考察により、隠れ部分群問題の従来主流となっている定式化についてやや曖昧な点を見出した。その曖昧さを解消することで隠れ部分群問題の困難性をより精密に行う研究を現在継続中である。

３．現在までの達成度

②おおむね順調に進展している。

（理由）

本研究課題について、研究開始後に新たに得た知見を反映させる形で、応募時に想定していた研究手法とはやや異なるアプローチにより研究を進めているものの、大目的である隠れ部分群問題の困難性に対する新たな評価については最終年度までに一定の成果が得られる見通しである。

４．今後の研究の推進方策

残りの年度は本研究期間の最終年度なので、これまでに得た研究成果をとりまとめて国際論文誌での採録決定・公表を目指すとともに、これまでの研究成果を基盤とした隠れ部分群問題の困難性に対する分析を完了させ、成果発表を行う。具体的な成果発表方針としては、年度中に、国内の当該分野の学会における口頭発表の他、査読付き国際会議への投稿・採録決定と、国際論文誌への投稿を目指す。（実際の論文査読の状況に応じて、年度中に成果公表が可能であれば成果公表まで行いたい。）

５． 代表的な研究成果
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計９件）

① 縫田光司, 「量子力学の物理原理的特徴付けと凸集合の幾何学」, 北海道大学数学講究録, 148 号, 59 頁～66 頁, 2011 年, 査読無
② Gen Kimura, Koji Nuida, Hideki Imai, ″Distinguishability measures and entropies for general probabilistic theories″, Reports on Mathematical Physics, vol.66, pp.175-206, 2010, 査読有
③ Koji Nuida, Gen Kimura, Takayuki Miyadera, ″Optimal observables for minimum-error state discrimination in general probabilistic theories″, Journal of Mathematical Physics, vol.51, 093505, 2010, 査読有
④ 縫田光司, 「量子計算、量子アルゴリズムと有限群の表現論」, 2009 年度表現論シンポジウム講演集, 74 頁～85 頁, 2009 年, 査読無
⑤ 縫田光司, 「一般確率モデルから眺める量子情報理論」, 北海道大学数学講究録, 140 号, 37 頁～41 頁, 2009 年, 査読無

〔学会発表〕（計６件）

① 縫田光司, 量子力学の物理原理的特徴付けと凸集合の幾何学, 第 7 回数学総合若手研究集会, 2011 年 3 月 3 日, 北海道大学（札幌市）
② Koji Nuida, On derivation of qubit systems from physical principles, 14th Workshop on Quantum Information Processing, 2011 年 1 月 10 日, The Capella (Sentosa, Singapore)
③ 縫田光司, 「量子計算、量子アルゴリズムと有限群の表現論」, 2009 年度表現論シンポジウム, 2009 年 11 月 18 日, フェストーネ（沖縄県）
④ 縫田光司, On Two-State Discrimination Problems in Generic Probability Models, 2009 年暗号と情報セキュリティシンポジウム(SCIS2009), 2009 年 1 月 20 日, 大津プリンスホテル（滋賀県）
⑤ Koji Nuida, On Minimum-Error State Discrimination Problems in Generic Probability Models, The Twelfth Workshop on Quantum Information Processing (QIP 2009), 2009 年 1 月 14 日, Santa Fe Convention Center (NM, USA)